

РОЛЬ ІНТЕРПОЛУ У БОРОТЬБІ З КІБЕРТЕРОРИЗМОМ

Церковна Анна Андріївна,

студентка 2-го курсу магістратури факультету міжнародних
економічних відносин та туристичного бізнесу,
Харківський національний університет імені В. Н. Каразіна,
e-mail: annaazori@gmail.com

Актуальність обраної теми дослідження обумовлена тим, що інформаційні технології сьогодні проникають у всі сфери людської діяльності, в тому числі – стають зброєю у руках злочинців. Особливе місце серед кіберзлочинів посідає кібертероризм, який стає однією з основних загроз глобальній безпеці.

Метою даного дослідження є визначення місця Інтерполу у системі міжнародних структур, покликаних боротися із сучасними формами злочинності, зокрема із кібертероризмом.

Міжнародна організація кримінальної поліції (Інтерпол) координує зусилля національних поліцій країн-членів. Сендлер, Ерс та Ендерс у своєму спільному дослідженні підрахували, що за кожен долар США, вкладений у контртерористичну діяльність Інтерполу, країни-члени отримують в середньому 200 доларів США [4].

Ця незалежна міжнародна організація була створена в 1923 році з місією сприяння міжнародному співробітництву в боротьбі з міжнародними злочинами. В даний час Інтерпол включає 190 країн-членів. Інтерпол пов'язує правоохоронні органи, Національні центральні бюро країн-членів та власно Генеральний секретаріат Інтерполу у боротьбі з транснаціональною злочинністю та тероризмом. Зокрема, Інтерпол має на меті вирішення шести основних кримінальних проблем: корупція, наркотики та організована злочинність, фінансові та високотехнологічні злочини, втікачі, торгівля людьми та транснаціональний тероризм [2].

Інтерпол підтверджує, що глобальна загроза тероризму сьогодні є неминучою і складнішою, ніж будь-коли. Зростаюча кількість конфліктних зон по всьому світу надає транснаціональним терористичним організаціям – таким, як ІГІЛ і Аль-Каїда – нові fronti, на яких вони можуть діяти одночасно. Також наявність та доступ до джерел, що пропагують насильство, розширюється на все більшій кількості мов, що змінило методику вербовки та радикалізації нових членів. Нинішнє покоління терористів також технологічно підковані й дуже активні у соціальних медіа. Комплексна система змін у пересуванні, підробці документів, далекоюсяжності та руйнівності атак, комунікаціях та маніпуляції соціальними мережами призвели до вирішального етапу у боротьбі з тероризмом, який вимагає всебічної скоординованої відповіді [1].

Генеральний секретаріат Інтерполу вирішив скоординувати досвід країн-членів у галузі Злочинності в сфері інформаційних технологій (англ. Information Technology Crime, ITC) через створення «робочої групи», тобто групи експертів. Такі робочі групи складаються з начальників чи досвідчених членів національних органів боротьби із комп'ютерною злочинністю, та покликані відображати регіональний досвід країн Європи, Азії, Південної та Північної Америки та Африки. Основним завданням центрального органу є гармонізація ініціатив різних регіональних робочих груп.

У вересні 2002 р., на тлі тривожного зростання кількості міжнародних терористичних атак, Інтерполом була створена так звана Об'єднана цільова група (англ. Fusion Task Force, FTF), направлена саме на боротьбу з міжнародним тероризмом. Основними її завданнями є виявлення активних терористичних груп та їх членів, збирання та обмін інформацією та розвідкою, надання аналітичної підтримки та посилення спроможності країн-членів щодо подолання загроз тероризму та організованої злочинності.

Усього було створено шість регіональних цільових груп у регіонах, що вважаються особливо сприйнятливими до терористичної діяльності: Проект Пасіфік (Південно-Східна Азія), Проект Калкан (Центральна Азія), Проект

Амазон (Південна Америка), Проект Баобаб (Африка), Проект Нексус (Європа) та Проект Близький Схід [5].

Значна роль Інтерполу у боротьбі з тероризмом визнана у всьому світі. У 2017 році Рада Безпеки ООН одноголосно прийняла Резолюцію 2396 про визнання зусиль Інтерполу у боротьбі з загрозою, яку представляють іноземні терористи, в тому числі шляхом глобального обміну інформацією між правоохоронними органами. В рамках своєї глобальної антитерористичної стратегії Інтерпол прагне протидіяти терористичним загрозам на цифрових платформах шляхом посилення можливостей аналізу соціальних медіа країн-членів в регіоні Близького Сходу, Північної Африки та в Пакистані.

14-16 січня 2019 року проходив спільний воркшоп, організований Інтерполом та Контртерористичним центром ООН, під назвою «Підвищення можливостей держав-членів щодо використання соціальних медіа для запобігання та протидії феномену іноземних терористичних винищувачів». Воркшоп зосереджувався на ролі правоохоронних органів для збору, аналізу та обміну інформацією, знайденою в Інтернеті, зокрема на платформах соціальних медіа, для сприяння виявленню, запобіганню, розслідуванню та кримінальному переслідуванню злочинів, пов'язаних з тероризмом. Учасники пройшли навчання з чотирьох основних напрямків: виявлення діяльності, пов'язаної з тероризмом в Інтернеті; збір електронних доказів; запит електронних доказів через кордон; та взаємодія з приватним сектором для просування розслідувань правоохоронними органами. Цей воркшоп є частиною більш широкого проекту щодо запобігання та боротьби з тероризмом на Близькому Сході, у Північній Африці, регіонах Південно-Східної та Південної Азії, який фінансується з Цільового фонду з питань боротьби з тероризмом. Цим фондом керує Управління боротьби з тероризмом ООН, уряд Японії та уряд ОАЕ [3].

Таким чином, Інтерпол визнає кібертероризм та застосування терористами сучасних технологій як важливу проблему, що повинна стояти на порядку денному усіх організацій у сфері міжнародної безпеки. В першу чергу, у боротьбі з кібертероризмом він займається координацією правоохоронних

органів країн-членів, наданням аналітичної інформації та проведенням освітніх заходів у цій сфері, що швидко змінюється та потребує постійного оновлення знань.

Список використаних джерел:

1. Counter-terrorism. Future-oriented policing projects. *Interpol Official Website*. URL: <https://www.interpol.int/content/download/5266/file/Counter-terrorism.pdf> (Last Accessed: 27.09.2019).
2. Gardezabal J., Sandler T. INTERPOL's Surveillance Network in Curbing Transnational Terrorism. *Journal of Policy Analysis and Management*. 2015. Vol. 34, No. 4. pp. 761–780.
3. INTERPOL and UN join forces to counter exploitation of Internet for terrorist activities. *Interpol Official website*. URL: <https://www.interpol.int/en/News-and-Events/News/2019/INTERPOL-and-UN-join-forces-to-counter-exploitation-of-Internet-for-terrorist-activities> (Last Accessed: 27.09.2019).
4. Sandler T., Arce D., Enders W. An evaluation of Interpol's cooperative-based counterterrorism linkages. *Journal of Law and Economics*. 2011. Vol. 54. pp. 79–110.
5. Tehrani P. M., Manap N. A., Taji H. Cyber terrorism challenges: The need for a global response to a multijurisdictional crime. *Computer Law & Security review*. 2013. Vol. 29. pp. 207–215.

Науковий керівник: Доценко Олена Михайлівна, доцент кафедри міжнародних відносин, міжнародної інформації та безпеки Харківського національного університету імені В. Н. Каразіна, канд. юрид. наук.